WHAT IS CLAIMED IS:

1. A seed generating circuit comprising:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data.

2. The seed generating circuit according to claim 1, wherein the oscillating circuit oscillates when a plurality of inputted data have a specific combination.

3. The seed generating circuit according to claim 2, wherein:

the oscillating circuit has two exclusive OR computing circuits and two inverter circuits coupled in series by turns, and

each of the plurality of inputted data is given to each of input ends of the two exclusive OR computing circuits, respectively.

4. The seed generating circuit according to claim 1, wherein the oscillating circuit includes a ring oscillating circuit, and the oscillating circuit oscillates continuously.

5. The seed generating circuit according to claim 1, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

6. The seed generating circuit according to claim 1, wherein appearance frequencies of "0" and "1" outputted from the smoothing circuit are more close to 1:1 than appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit.

7. The seed generating circuit according to claim 1, wherein the postprocessing circuit has an exclusive OR computing circuit which performs the computation.

8. The seed generating circuit according to claim 1, wherein the postprocessing circuit generates the one-bit seed based on a table which assigns either "0" and "1" corresponding

to a combination of the plurality of bits.

9. A random number generating circuit comprising:

the seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data.

10. The random number generating circuit according to claim 9, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated

by the pseudo random number generating circuit.

11. The random number generating circuit according to claim 9, wherein the postprocessing circuit has an exclusive OR computing circuit which performs the computation.

12. The random number generating circuit according to claim 9, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.

13. A semiconductor integrated circuit comprising a random number generating circuit having:

the seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the

digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data.

14. The semiconductor integrated circuit according to claim 13, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

15. The semiconductor integrated circuit according to claim 13, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.

16. An IC card comprising a semiconductor integrated circuit including a random number generating circuit having:

the seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data.

17. The IC card according to claim 16, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.

18. An information terminal equipment comprising the semiconductor integrated circuit including a random number generating circuit having:

the seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data.

19. The information terminal equipment according to claim 18, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

20. The information terminal equipment according to claim 18, further comprising a uncertain logic circuit which

gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.